CSCE 585 Project
Milestone P2
Intelligent In-Network Attack Detection

Sergio Elizalde, Amith GSPN, Samia Choueiri

Department of Integrated Information Technology
University of South Carolina

December 2, 2025

Problem and motivation

Cyberattacks are evolving, and more intelligent approaches are needed

- Traditional defenses alone are no longer sufficient, requiring adaptive and AI-driven security solutions.

Network speed is increasing, raising the need for in-network acceleration

- As data volumes grow, systems must process and respond in real time to keep pace with modern demands.

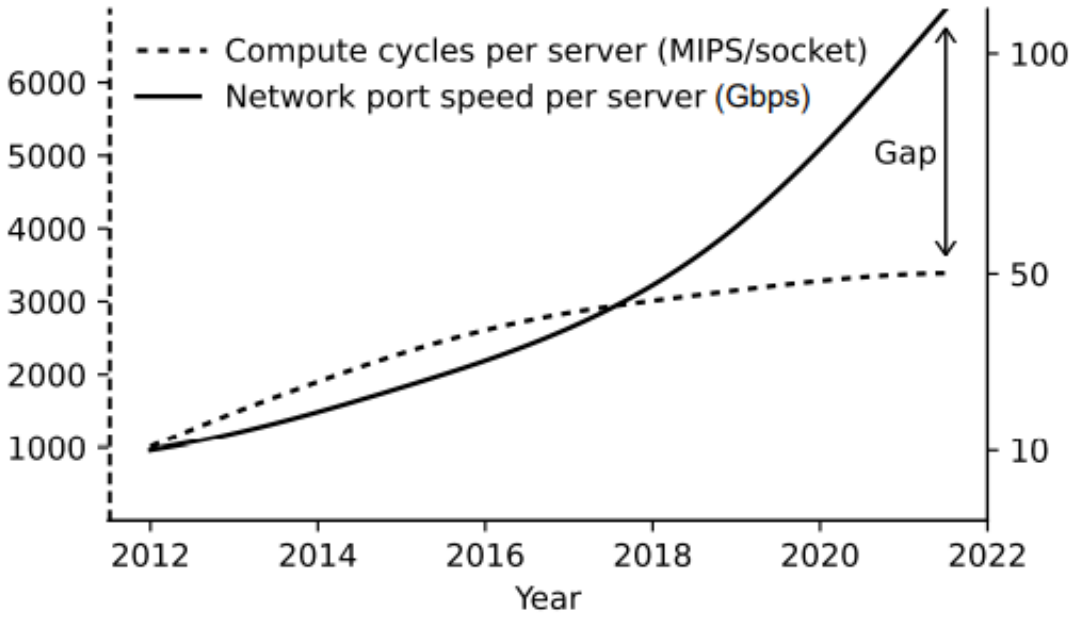


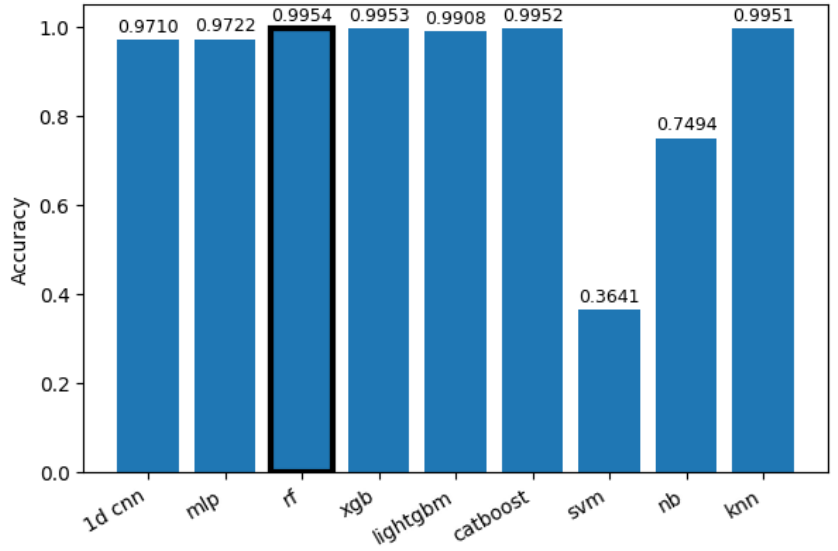
Figure: G. Elinoff, “Data centers are overloaded. The inventor of FPGAs is swooping in with a “comprehensive” SmartNIC,” March 2020.

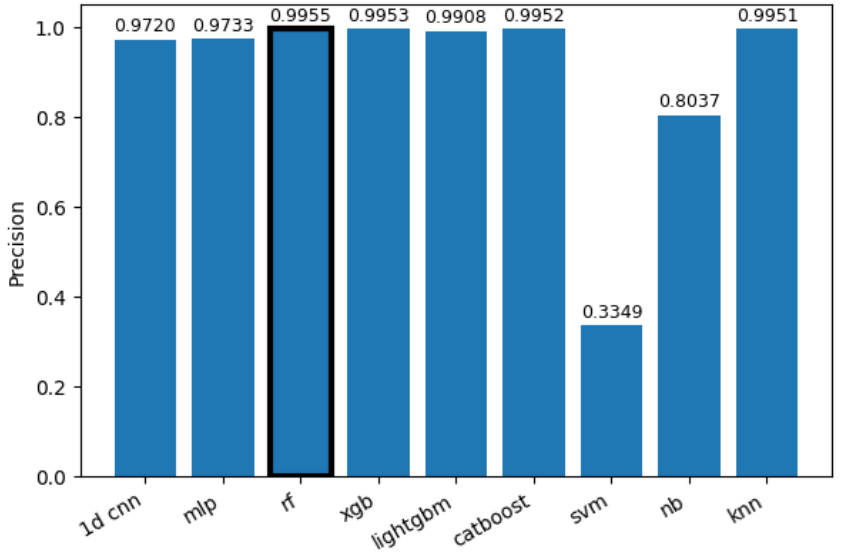
Methods

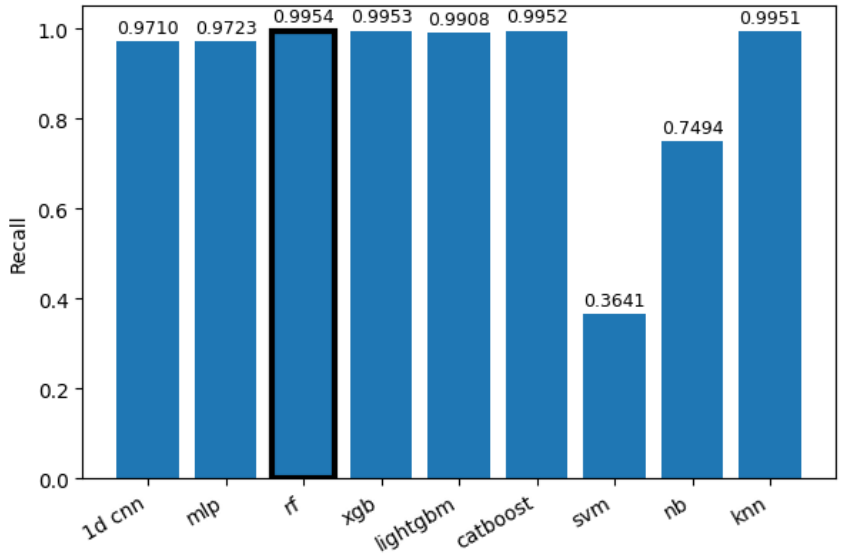
- Dataset: CIC-IDS2017[1]
- Offline:
  - ML models: Multilayer Perceptron (MLP), 1D Convolutional Neural Network (1D-CNN), Random Forest (RF), XGBoost (XGB), LightGBM (LGBM), CatBoost (CB), Support Vector Machine (SVM), Gaussian Naïve Bayes (GNB), and K-Nearest Neighbors (KNN).
  - Classification report: Global Accuracy, Precision, Recall and F1-score.
  - Feature importance.
- Online:
  - ML model: Random Forest.
  - Classification report: Global Accuracy, Precision, Recall and F1-score.
  - Latency of packet processing.
  - Throughput.

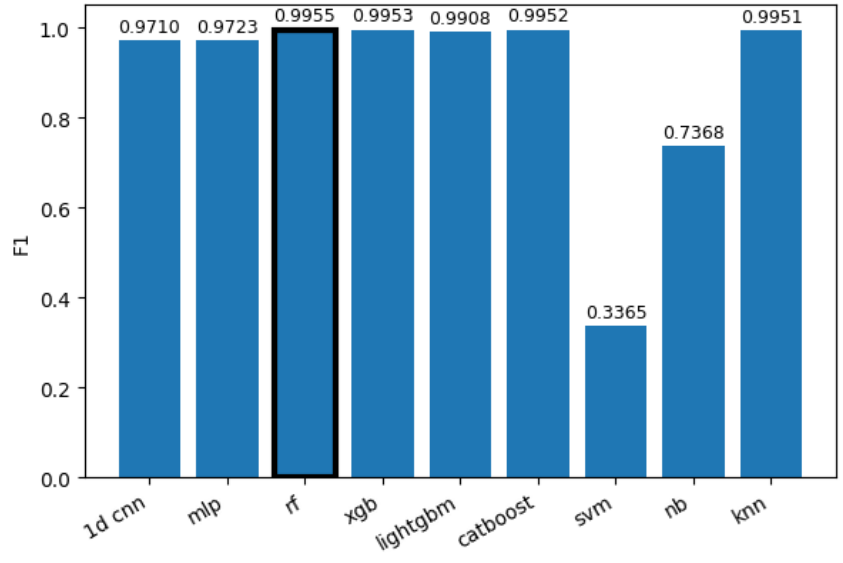
1. Sharafaldin, Iman, Arash Habibi Lashkari, and Ali A. Ghorbani. "Toward generating a new intrusion detection dataset and intrusion traffic characterization." ICISSp 1.2018 (2018): 108-116.

Offline Training Results

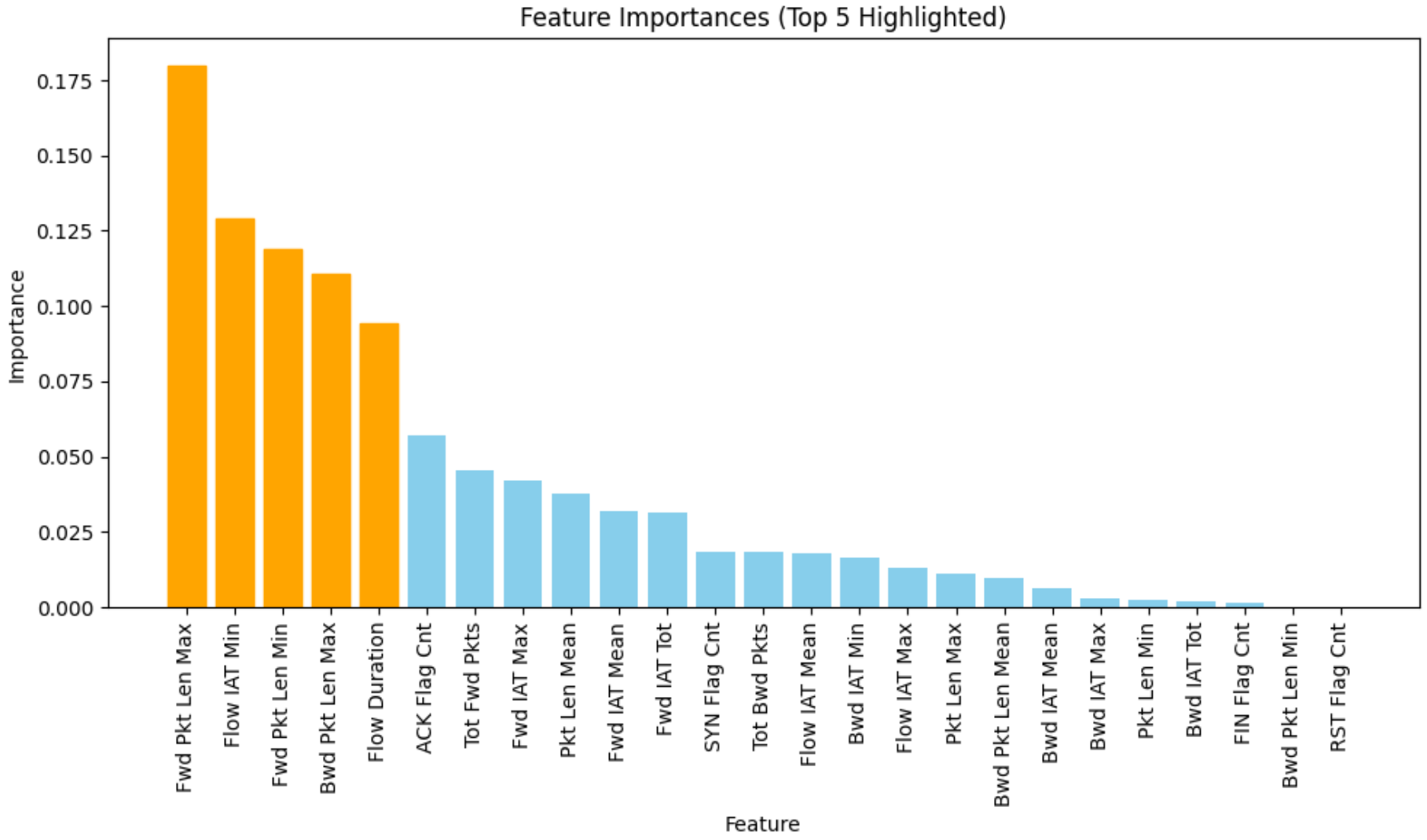






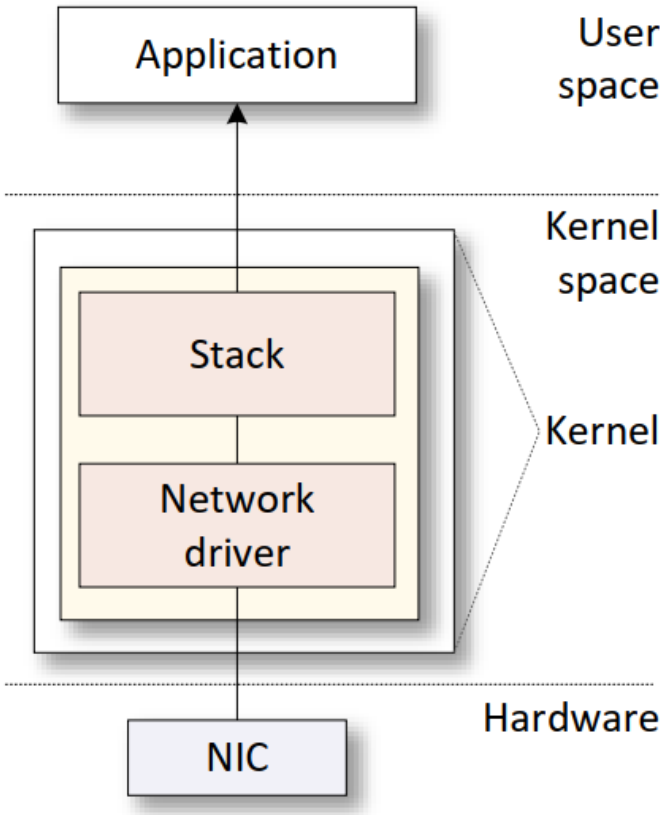


Offline Feature Importance



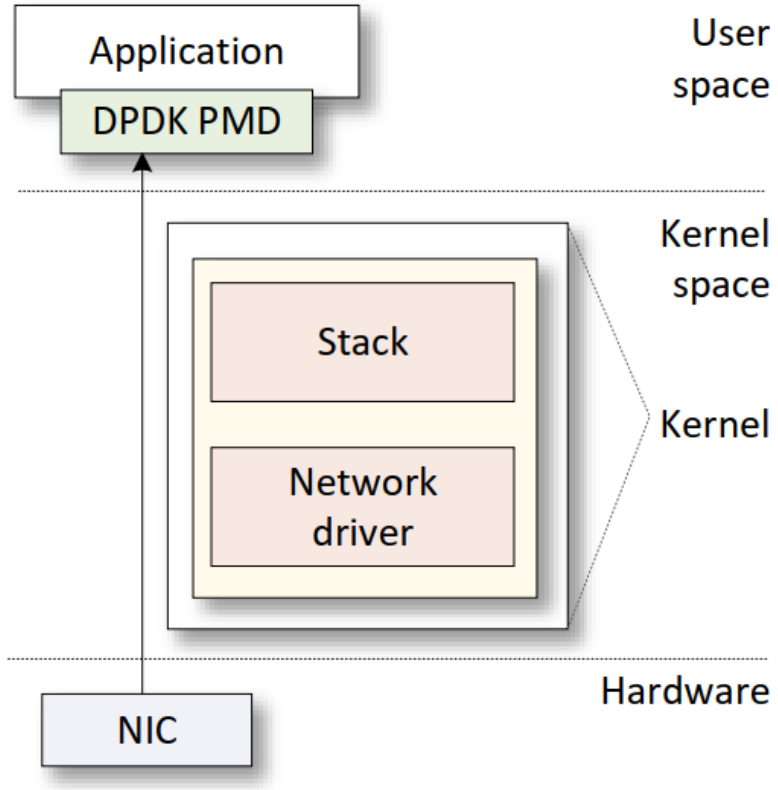
Standard Packet Processing

- The Network Interface Card (NIC) driver pre-allocates kernel memory buffers where the packets are stored.
- The NIC driver pre-allocate the transmit (TX) and receive (RX) ring buffer in the memory.
- The ring buffers store the packet buffer pointer and its length.
- The NIC copies the packet to the location using Direct Memory Access (DMA).
- The NIC triggers an interrupt.



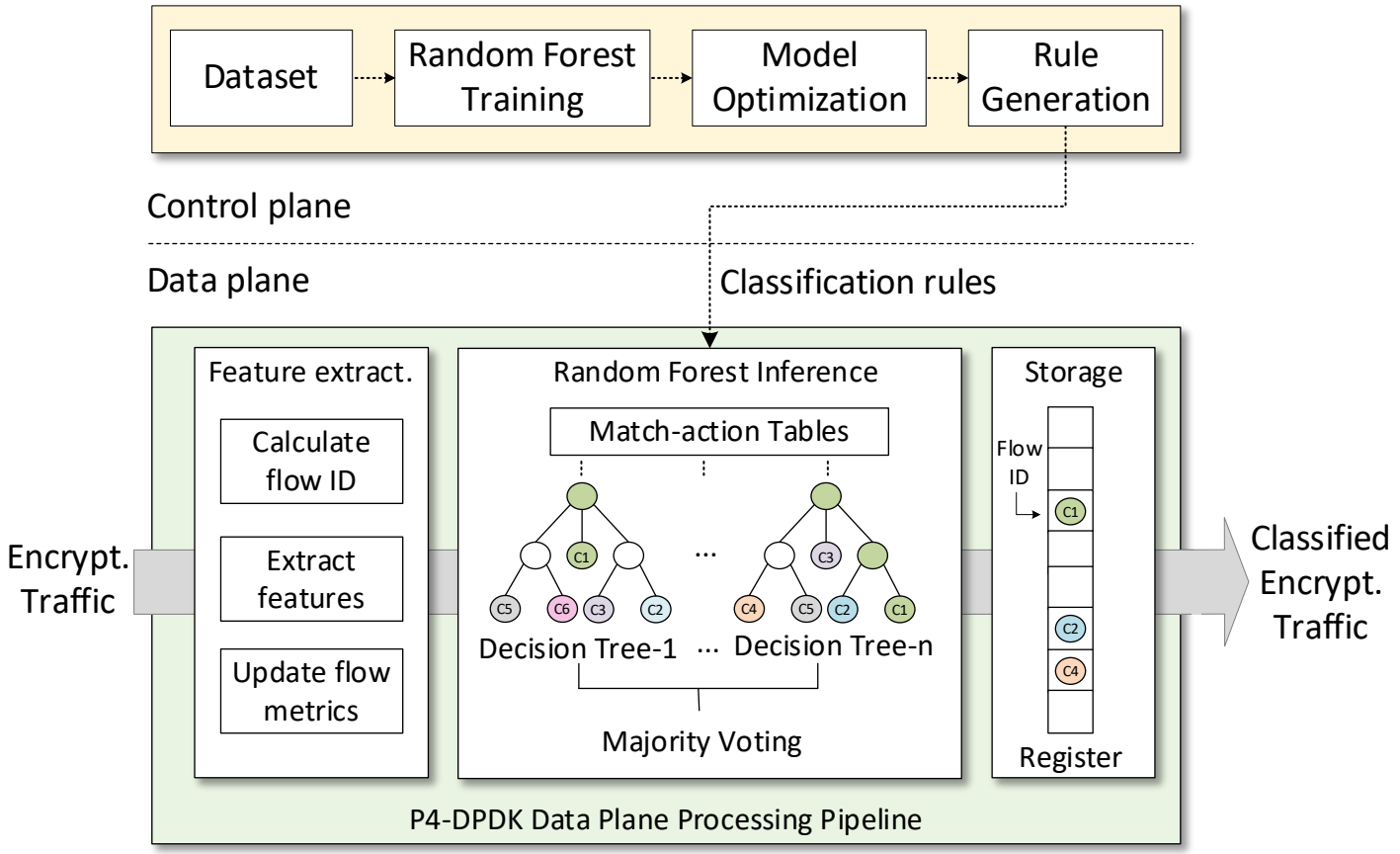
Kernel-Bypass Packet Processing Using DPDK

- Bypassing the kernel is a solution to avoid kernel overheads and accelerate packet processing.
- DPDK is a set of optimized libraries for processing packets in the user space while bypassing the kernel.
- DPDK uses Poll Mode Drivers (PMD) which constantly poll the NICs for new packets to avoid overheads resulting from interrupts.

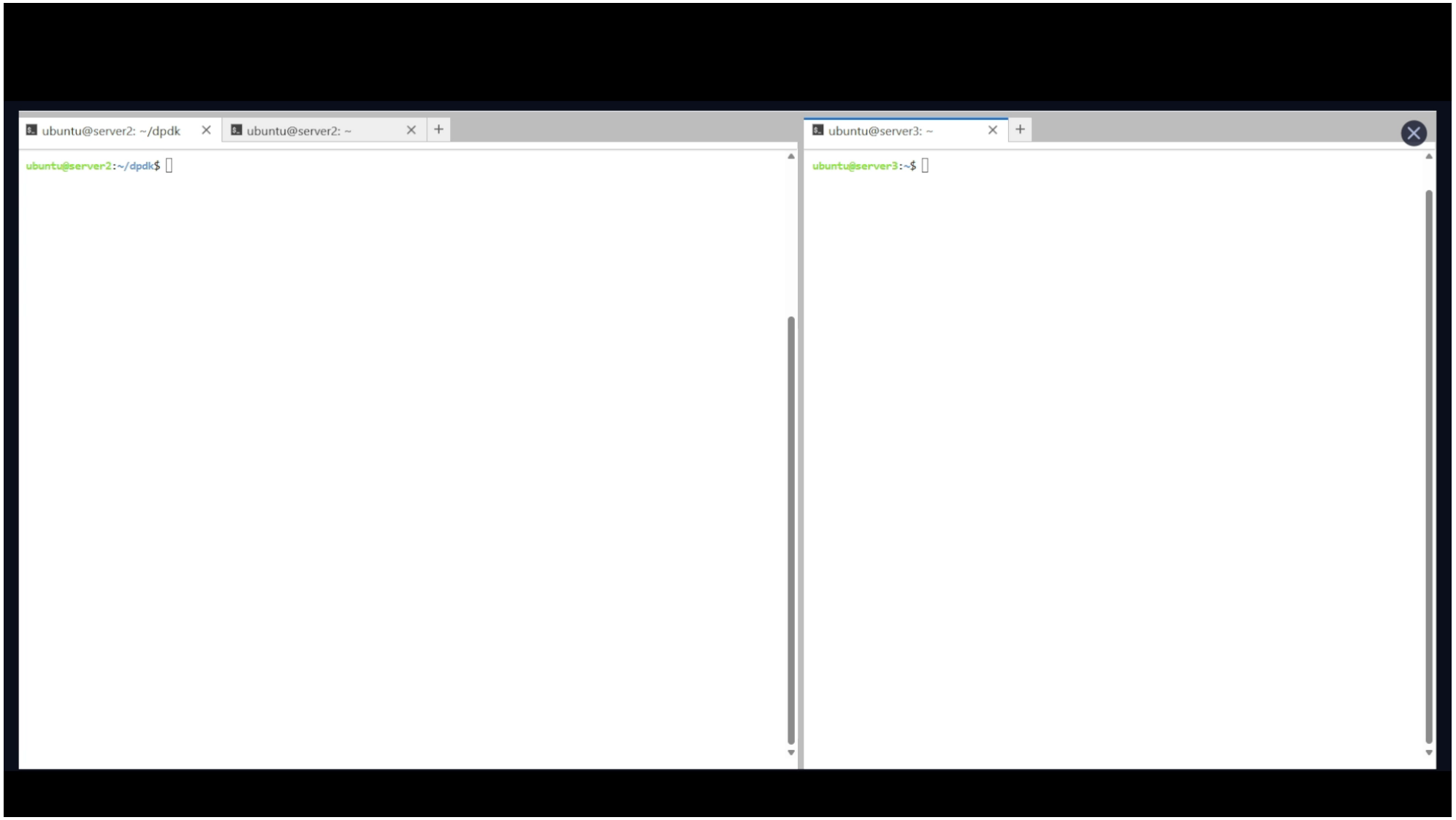


Proposed System

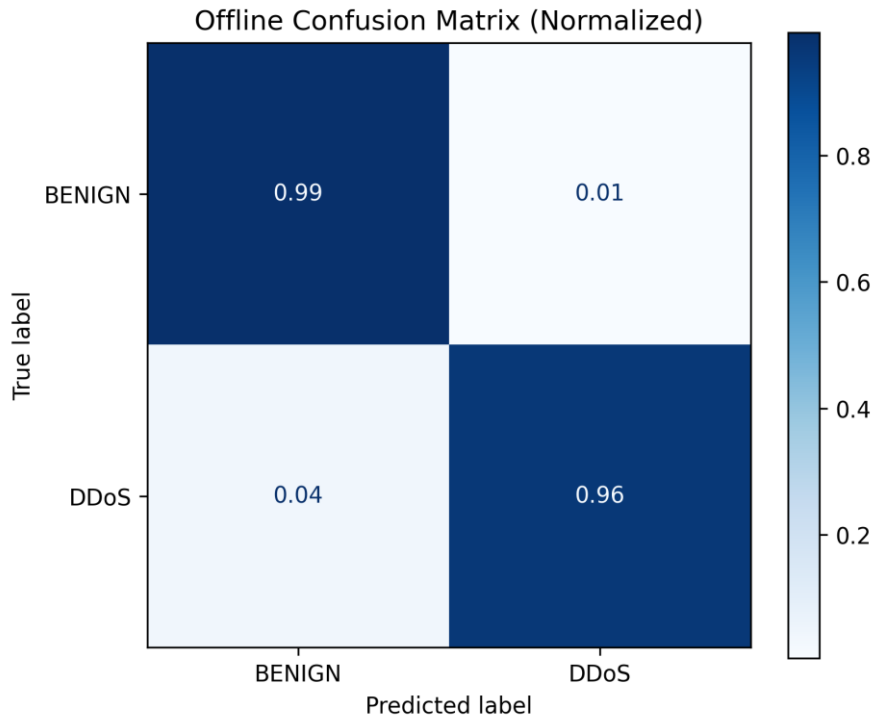
- The control plane is responsible of training the model offline.
- The system uses Random Forest to classify live traffic.
- The control plane, converts trained models into classification rules for deployment in the data plane.
- The data plane is responsible of extracting the features, implementing the trained model and storing the results.

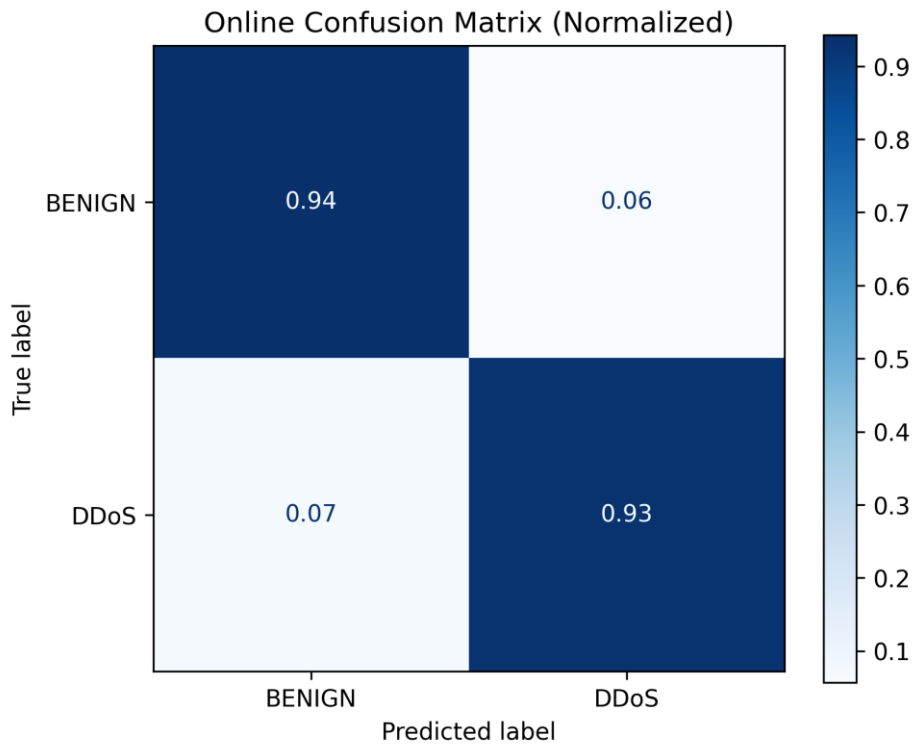


Demo


ubuntu@server2: ~/dpdk
ubuntu@server2: ~
ubuntu@server2:~/dpdk$
ubuntu@server3: ~
ubuntu@server3:~$

Training Results





Discussion and Future Work

- Limitations:
  - Depth of the tree is limited by the architecture of P4-DPDK
  - There is no division and multiplication, it means no complex features are feasible (e.g., Standard Deviation).
  - The system does not implement mitigation (e.g., drop or rate limit)
  - Evasion attacks are not considered during training

- Future work:
  - Train multiclass random forest
  - Add adversarial samples
  - Accelerate inference with parallel instructions (e.g., SIMD)
  - Extend to other datasets and cyberattacks

THANK YOU!